THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

18 U.S.C. § 2510. Definitions:

(4) "intercept" means the . . . acquisition of the contents of any . . . electronic . . . communication through the use of any electronic . . . device;

(5) "electronic . . . device" means any device or apparatus which can be used to intercept a . . . electronic communication . . . .;

(6) "person" means any . . . individual, partnership, association, joint stock company, trust, or corporation;

(11) "aggrieved person" means a person who was a party to any intercepted . . . electronic communication or a person against whom the interception was directed;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive . . . electronic communication;

(17) "electronic storage" means-

(A) any temporary, intermediate storage of . . . electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; . . . .

18 U.S.C. § 2511(1) Except as otherwise specifically provided in this chapter any person who-

(a) intentionally . . . procures any other person to intercept . . . , any . . . electronic communication;

(c) intentionally discloses, . . . to any person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through interception of . . . electronic communication in violation of this subsection . . . shall be punished. . . .

18 U.S.C. § 2511(2)(a)(i) . . . except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

18 U.S.C. § 2511(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

18 U.S.C. § 2516(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may

grant, in conformity with section 2518 of this title, or order authorizing or approving the interception of electronic communication by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made when such interception may provide or has provided evidence of any Federal felony.

18 U.S.C. § 2518(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, especially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute or that State, who reasonably determines that-

(a) an emergency situation exists that involves-

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interests, or

(iii) conspiratorial activities characteristic of organized crime.

that requires . . . electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such . . . electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has

occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for approval is denied, or in any other case earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any . . . electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

18 U.S.C. § 2520(a) In general.-Except as provided in section 2511(2)(a)(ii), any person whose . . . electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief may be appropriate.

(d) Defense.-A good faith reliance on-

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of; is a

complete defense against any civil or criminal action brought under this chapter or any other law.

18 U.S.C. § 2702. (a) **Prohibitions.**- Except as provided in subsection (b)-

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service;. . .

(b) **Exceptions.**-A person or entity may divulge the contents of a communication-

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, . . .: or

(6) to a law enforcement agency, is such contents-

(A) were inadvertently obtained by the service provider; and

(B) appear to pertain to the commission of a crime.

18 U.S.C. § 2703. **Requirements of government access**

(a) **Contents of electronic communications in electronic storage.**- A Government entity may require the disclosure by a provider of electronic communication service of the contents of an electronic

communication, that is in electronic storage in an electronic communication system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedures or equivalent State warrant. A government entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(c) **Records concerning electronic service** . . . .

(B) A provider of electronic communication service . . . shall disclose a record or other information pertaining to a . . . customer of such service (not including the contents of communications covered by subsection (a)(b) of this section) to a government entity only when the government entity-

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena;

(ii) obtains a warrant issued under the Federal Rules of Criminal Procedures or equivalent State warrant;

(iii) obtains a court order for such disclosure under subsection (d) of this section; or

(iv) has the consent of the . . . customer to such disclosure.

(e) **No cause of action against a provider disclosing information under this chapter.**-No cause of action shall

lie in any court against any provider of . . . electronic communication service, its officer, employee, agents, or other specified persons for providing information, facilities, or assistance with the terms of a court order, warrant, subpoena, or certification under this chapter.

18 U.S.C. § 2707. Cause of action

(a) Cause of action- Except as provided in section 2703(e), any . . . customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

(d) Defense.-A good faith reliance on-

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law

18 U.S.C. § 2711. Definitions for chapter

As used in this chapter-

(1) the terms defined in section 2510 of this title have, respectively, the definitions given in that section.